Mit Sicherheit innovativ.

An alle Bieter

Bundesrechenzentrum GmbH
Hintere Zollamtsstraße 4
1030 Wien, Austria

Sabrina Radosavljevic
ausschreibung.k-er-be@brz.gv.at
+43-1-711 23-88 24 70

Wien, 9. Mai 2018

Betreff: Vergabeverfahren SEC2018, GZ. 7.1.1/0021-K-ER-BE/2018
Beantwortung von Rückfragen zu den Ausschreibungsunterlagen der 1. Stufe und Berichtigung

Sehr geehrte Damen und Herren!

In obiger Angelegenheit finden Sie nachstehend die schriftliche Beantwortung von Rückfragen gemäß Teil A "Bestimmungen für den Teilnahmeantrag zur Auswahl geeigneter Bewerber", Punkt 18 und eine Berichtigung der Teilnahmeunterlagen in den Teilen A, Bestimmungen für den Teilnahmeantrag zur Auswahl geeigneter Bewerber und in den Teil C-1 und C-2, Formblätter zum Nachweis der technischen Leistungsfähigkeit für die Teilleistung 1 und 2:

I. Rückfragenbeantwortung

Frage 1:

Unter Punkt 21.5.5 Sicherheitsüberprüfung der nominierten Schlüsselpersonen für TL 1 und TL 2 muss der Bewerber sicherstellen, dass für sämtliche von ihm namhaft gemachten Personen gemäß den Punkten 21.5.2 und 21.5.4, die für die Erbringung der gegenständlich angebotenen Leistungen herangezogen werden sollen, eine gültige und positiv bestandene Sicherheitsüberprüfung gemäß §§ 55ff SPG der Stufe "vertraulich", „geheim“ oder „streng geheim“ vorliegt oder nach Aufforderung durch den Auftraggeber eingeholt wird.

Wir können für unsere Mitarbeiterinnen/Mitarbeiter unterschiedliche europäische Sicherheitsüberprüfungen nachweisen. Kann daher beispielsweise die erweiterte Sicherheitsüberprüfung („Ü2“) nach § 9 SÜG (Sicherheitsüberprüfungsgesetz der Bundesrepublik Deutschland) bzw. EU-Confidential als gleichwertig mit §§55 SPG angesetzt werden?

Antwort:

Überprüfungen gemäß § 55 SPG erfolgen durch das österreichische Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) auf Basis österreichischen Rechts. Sicherheitsüberprüfungen anderer Länder können daher nicht als gleichwertig angesehen werden.

Frage 2:

Bei den Teilleistungen 1 und 2 wird jeweils unter dem Kriterium „Anzahl und Qualifikation des Schlüsselpersonals“ bei Merkmal 3 eine Personenzertifizierung gefordert bzw. bei nicht vorhanden sein eine aufrechte Zertifizierung als CISSP (Certified Information Systems Security Professional) des International Information System Security Certification Consortium (ISC2) als gleichwertig angesehen.

Können bei diesem Merkmal auch Abschlüsse von einschlägigen technischen Universitäten bzw. andere als die genannten Zertifikate als gleichwertig angesetzt werden?

Antwort:

Ein entsprechender Universitätsabschluss wird sowohl für Teilleistung 1 als auch Teilleistung 2 nicht als gleichwertig angesehen, da die geforderten Qualifikationen auch entsprechende Erfahrungen betreffend die angeführten Tätigkeiten voraussetzen.

In diesem Zusammenhang wird aber auch auf die Beantwortung der Frage 18 verwiesen.

Frage 3:

Gemäß Pkt 21.5.1. ist die Nennung von Referenzaufträgen mit Angabe des Auftraggebers und rechtsgültiger Zeichnung zu bestätigen bzw. mittels Eidesstattlicher Erklärung zu bestätigen. Ist die namentliche Bekanntmachung des Referenzauftraggebers verpflichtend? Bzw. welche Daten des Referenzauftraggebers sind verpflichtend anzuführen?

Antwort:

Es sind sämtliche in den Formblättern geforderte Information anzugeben und daher sind grundsätzliche alle Felder in den Formblättern auszufüllen. Sollte z.B. aufgrund von Vertraulichkeitsverpflichtungen die namentliche Nennung des Referenzauftraggebers nachweislich nicht möglich sein, kann die namentliche Nennung unterbleiben.

Weiters gilt in diesem Fall folgende Regelung laut Teil A bzw. den jeweiligen Formblättern: Sollte eine Bestätigung durch den Referenzauftraggeber nicht erlangt werden können, reicht eine diesbezügliche eidesstattliche Erklärung laut beiliegendem Muster des Bewerbers/Federführers der Bewerbergemeinschaft, dass die Angaben richtig sind und die Leistung vom Referenzauftragnehmer fachgerecht und ordnungsgemäß durchgeführt wurde. Diese eidesstattliche Erklärung hat auf einem Ergänzungsblatt zu erfolgen.

Frage 4:

Ist es zulässig die Leistungen für Teilleistung 1: Technische Sicherheitsaudits teilweise remote (d.h. aus anderen Ländern aus dem EU-Raum) zu erbringen?

Antwort:

Gemäß Teil A, Punkt 5.2.2 a) sind Technische Sicherheitsaudits grundsätzlich am Standort der Bundesrechenzentrum GmbH in 1030 Wien, Hintere Zollamtsstraße 4, durchzuführen. Sollte ein Audit von einem anderen Standort aus stattfinden, so ist dies im Zuge der Auditplanung abzustimmen und gesondert festzulegen.

Frage 5:

Ist es zulässig die Leistungen für Teilleistung 2: Penetrationstests teilweise remote (d.h. aus anderen Ländern aus dem EU-Raum) zu erbringen?

Antwort:

Gemäß Teil A, Punkt 5.3.2 a) sind Penetrationstests am Standort der Bundesrechenzentrum GmbH in 1030 Wien, Hintere Zollamtsstraße 4, durchzuführen. Sollte ein Penetrationstest (z.B. ein Blackbox-Penetrationstest) von einem anderen Standort aus durchgeführt werden (z.B. vom Firmensitz des Auftragnehmers), so ist dies im Zuge der Auditplanung abzustimmen und gesondert

festzulegen. Wir weisen darauf hin, dass in den Ausschreibungsunterlagen festgelegt ist, dass die Tests jedenfalls von einem Standort in der europäischen Union durchgeführt werden müssen.

Frage 6:

Betreffend Teil A Bestimmungen für den Teilnahmeantrag: Gem. Ziffer 2.1 des Teil A Bestimmungen für den Teilnahmeantrag soll das Vergabeverfahren als offenes Verfahren gem. § 25 Abs. 2 BVergG in Form eines Preisangebotsverfahrens (§ 2 Z 27 BVergG ivm § 24 Abs.1 BvergG) geführt werden. In Ziffer 3.1. des Teil A Bestimmungen für den Teilnahmeantrag wird jedoch das Verfahren als Verhandlungsverfahren mit vorheriger Bekanntmachung gemäß § 30 Abs 1 Z 3 BVergG 2006 mit verkürzter Teilnahmefrist aufgrund Verwendung elektronischer Medien gemäß § 62 Abs 1 Z 2 BVergG 2006 im Oberschwellenbereich des BVergG 2006 (§ 12 Abs 1 Z 1 BVergG 2006) als Preisangebotsverfahren (§ 2 Z 27 BVergG) gemäß § 24 Abs 1 BVergG 2006 zum Abschluss einer Rahmenvereinbarung gemäß §§ 150 ff BVergG 2006 mit mehreren Unternehmen bestimmt und in den weiteren Unterlagen das Verfahren ebenfalls wie letztgenannt beschrieben.

Gehen wir daher richtigerweise davon aus, dass die Verfahrensart ein Verhandlungsverfahren mit vorheriger Bekanntmachung gemäß § 30 Abs 1 Z 3 BVergG 2006 mit verkürzter Teilnahmefrist aufgrund Verwendung elektronischer Medien gemäß § 62 Abs 1 Z 2 BVergG 2006 im Oberschwellenbereich des BVergG 2006 (§ 12 Abs 1 Z 1 BVergG 2006) als Preisangebotsverfahren (§ 2 Z 27 BVergG) gemäß § 24 Abs 1 BVergG 2006 zum Abschluss einer Rahmenvereinbarung gemäß §§ 150 ff BVergG 2006 mit mehreren Unternehmen bestimmt ist und eine Verhandlung auch über die Vertragsbedingungen stattfindet?

Antwort:

Die Regelung „Das Vergabeverfahren wird als offenes Verfahren gemäß § 25 Abs 2 BVergG in Form eines Preisangebotsverfahren (§ 2 Z 27 BVergG iVm § 24 Abs 1 BVergG) zum Abschluss von Rahmenvereinbarungen mit mehreren Unternehmern geführt.“ in Punkt 2.1, Teil Bestimmungen für den Teilnahmeantrag ist irrtümlich in den Ausschreibungsunterlagen enthalten und kommt daher nicht zur Anwendung. Die Teilnahmeunterlagen werden entsprechend berichtigt.

Frage 7:

Betreffend Teil A Bestimmungen für den Teilnahmeantrag: Gehen wir richtigerweise davon aus, dass für die Klärung und Vorgabe der zu beachtenden rechtlichen und regulatorischen Anforderungen insbesondere im Hinblick auf die z.B. datenschutzrechtlichen oder sonstigen Anforderungen bezüglich der Leistungsumsetzung, sowie die Anpassungen durch gesetzliche bzw. betriebliche Anforderungen der Auftraggeber verantwortlich ist? Sodass dementsprechend insbesondere auch die Auditkriterien und die inhaltliche Ausgestaltung des Audits betreffend Ziffer 5.2.2 a) des Teil A Bestimmungen für den Teilnahmeantrag – das heißt die Richtlinien, Standards, Prozesse, Vorgehensweisen und Anforderungen, letztverantwortlich durch dem Auftraggeber bestimmt werden und dementsprechend auch das Bewertungsschema gem. Ziffer 5.2.2 b) des Teil A Bestimmungen für den Teilnahmeantrag letztverantwortlich vom Auftraggeber vorgegeben wird, sowie auch die Festlegung der Testkriterien und die inhaltliche Ausgestaltung des Penetrationstest und die Prüfung und Sicherstellung der rechtlichen Zulässigkeit des Selbigen (siehe auch Ziffer 5.3.2 a) in der Verantwortung des Auftraggebers liegen?

Antwort:

Nein. Jeder Auftragnehmer ist selbstverständlich für die rechtskonforme Erbringung der eigenen Leistungen verantwortlich und hat daher auch die Vorgaben der Europäischen Union und die österreichischen Vorgaben zum Datenschutz zu beachten.

Frage 8:

Betreffend Teil B Bewerbererklärung: Gehen wir richtigerweise davon aus, dass die Einhaltung der Datenschutzvorschriften gem. Ziffer 0.5 Bewerbererklärung nur die Pflichten des Bewerbers umfassen, die Ihn als Auftragsverarbeiter treffen?

Antwort:

Geeignete Bieter sind dazu verpflichtet die gesetzlichen und EU-rechtlichen Datenschutzvorgaben nicht nur in der Rolle als Auftragsverarbeiter einzuhalten. Es wird in diesem Zusammenhang auf Punkt 22.1 (Berufliche Zuverlässigkeit) des Teils A, Bestimmungen für den Teilnahmeantrag hingewiesen.

Frage 9:

Wir gehen davon aus das wir bei den Referenzaufträgen für die Teilleistung 2 sowohl Blackbox als auch Whitebox auswählen können, wenn bei dem Referenzauftrag zuerst ein Blackbox und als zweiter Schritt ein Whitebox-Pentrationtest durchgeführt wurde.

Antwort:

Ja, das ist korrekt.

Frage 10:

Setzt ein Whitebox-Penetrationtest bei den Referenzaufträgen für die Teilleistung 2 einen Static Application Security Testing (SAST) bzw. einen manuellen Code-Review voraus?

Antwort:

Die Durchführung von Static Application Security Testing (SAST) bzw. manuellen Code-Reviews ist keine Voraussetzung für einen Whitebox-Penetrationtest als Basis zur Nennung bei den Referenzaufträgen.

Frage 11:

Wird die toolunterstützte SAST Produkthersteller Lösung von BRZ eingeschränkt oder kann der Anbieter das SAST Produkt auswählen?

Antwort:

Die Auswahl des/der Tools erfolgt grundsätzlich im Einvernehmen zwischen dem Auftraggeber und dem Auftragnehmer. Die BRZ GmbH geht jedenfalls davon aus, dass der Anbieter zur Durchführung entsprechender Tests Produkte von namhaften Herstellern einsetzt und hierfür auch bereits eine entsprechende Erfahrung vorliegt.

Frage 12:

Übernimmt der Auftraggeber bei toolunterstützten SAST anfallende Lizenzkosten?

Antwort:

Aus heutiger Sicht wird folgende Regelung angedacht: Im Rahmen der Abstimmung zum Abruf von Leistungen sollen im Falle eines Whitebox Penetration Tests mit Static Application Security Testing

(SAST) etwaige Lizenzkosten durch den Auftragnehmer entsprechend angeführt werden und diese werden in so einem Fall nach erfolgter Abstimmung mit dem Auftraggeber voraussichtlich übernommen. Diesbezügliche Details werden in den Ausschreibungsunterlagen der zweiten Stufe geregelt.

Frage 13:

Verwendet der Auftraggeber bereits eine toolunterstützte SAST Lösung und wird diese bei einem Whitebox-Penetrationtest mit SAST Erweiterung zu Verfügung gestellt.

Antwort:

Da die Nutzung entsprechender Tools sowie die Verifizierung von Findings entsprechendes Wissen und Erfahrung voraussetzt, wird davon ausgegangen, dass die besten Ergebnisse mit jenem Tool / jenen Tools erzielt werden, mit welchem / welchen der Auftragnehmer bereits einschlägige Erfahrungen besitzt. Dementsprechend wird grundsätzlich für entsprechende Tests kein Tool von Seiten der BRZ GmbH zur Verfügung gestellt.

Frage 14:

Ist für jede Schlüsselperson ein Skillprofil erforderlich oder ist ein Lebenslauf ausreichend?

Antwort:

Gemäß Teil A, Punkt 21.5.2.3 bzw. 21.5.4.3 ist für jede namhaft gemachte Schlüsselperson ein Skillprofil mit dem Ausbildungsschwerpunkt und der beruflichen Laufbahn samt Beschreibung der Berufstätigkeiten beizulegen. In diesen Zusammenhang wird auch auf die Frage 16 und deren Beantwortung verwiesen.

Frage 15:

Ist für jede Schlüsselperson ein Dienstzeugnis erforderlich?

Antwort:

Gemäß Teil A, Punkt 21.5.2.3 bzw. 21.5.4.3 ist die Berufserfahrung jeder namhaft gemachten Schlüsselperson durch entsprechende Verwendungszeugnisse (z.B. Dienstzeugnisse) nachzuweisen.

Frage 16:

Was versteht man unter einem Skillprofil? Ist ein Skillprofil mit einem Lebenslauf zu vergleichen?

Antwort:

Grundsätzlich ja, wobei hinsichtlich der Inhalte auf Teil A, Punkt 21.5.2.3 bzw. 21.5.4.3 verwiesen wird.

Frage 17:

21.5.2.1. & 2 Merkmal 2: Was passiert wenn MitarbeiterInnen nicht 35 Stunden sondern nur 30/32 Stunden angestellt sind?

Antwort:

Die Teilnahmeunterlagen werden berichtigt, sodass Merkmal 2 auch dann erfüllt ist, wenn die nominierte Schlüsselperson unter anderem ein aufrechtes Dienst- / Vertragsverhältnis (ist Angestellte/r gem. AngG oder Beschäftigte/r mit einem freien Dienstvertrag oder Werkvertrag), im Ausmaß von zumindest 30 Wochenstunden hat.

Frage 18:

21.5.2.1 & 2 Merkmal 3: Gilt das CISA Zertifikat als gleichwertig?

Antwort:

Gilt ausschließlich für Teilleistung 1:

Die Anforderung, dass ein Zertifikat einer akkreditierten Stelle für Personenzertifizierungen (Basis ISO 17024) oder eine Zertifizierung als CISSP vorliegen muss gewährleistet ein entsprechendes Qualitätsniveau als auch technisches und organisatorisches Wissen im Bereich unterschiedlicher Wissensdomänen im Bereich der Informationssicherheit.

Eine aufrechte Zertifizierung als Certified Information Systems Auditor (CISA) der Information Systems Audit and Control Association (ISACA)[1] wird als gleichwertig angesehen.

Gilt ausschließlich für Teilleistung 2:

Es werden keine anderen außer jenen in Teil A, Punkt 21.5.4 Merkmal 3 ausdrücklich angeführten Zertifizierungen anerkannt.

[1] www.isaca.org

II. Berichtigung der Ausschreibungsunterlagen

Die Bundesrechenzentrum GmbH teilt Ihnen mit, dass die Teilnahmeunterlagen des Vergabeverfahrens SEC2018 mit der Geschäftszahl 7.1.1/0021-K-ER-BE/2018 gemäß § 90 BVergG berichtigt werden.

Die berichtigten Ausschreibungsunterlagen sind von der Homepage des Auftraggebers (www.brz.gv.at → „Laufende Vergabeverfahren“ → „Bewerberauswahl/ Verhandlungsverfahren“) herunterzuladen und von den Bewerbern Ihren Teilnahmeanträgen verpflichtend zugrunde zu legen. Die berichtigten Bestimmungen sind in den Teilnahmeunterlagen im Überarbeitungsmodus (Markup) ersichtlich gemacht.

Bei der gegenständlichen Berichtigung handelt es sich um eine geringfügige Modifizierung, die naturgemäß keinerlei Einfluss auf die Teilnahmefrist hat.

Die Bieter werden aufgefordert, obige Antworten und Berichtigungen bei Erstellung ihrer Teilnahmeanträge zu berücksichtigen.

Mit freundlichen Grüßen

BRZ	**Unterzeichner**	i.V. Sabine Koller
	Datum/Zeit-UTC	2018-05-09T13:52:48+02:00
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 ("eIDAS-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.	
Prüfinformation	Informationen zur Prüfung finden Sie unter http://www.signaturpruefung.gv.at	

Mag.[a] Sabine Koller, MSc
Leiterin Beschaffung